

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-84278
(P2002-84278A)

(43) 公開日 平成14年3月22日 (2002.3.22)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 12/24		H 0 4 M 3/36	A 5 K 0 1 9
12/26		H 0 4 L 11/08	5 K 0 3 0
H 0 4 M 3/36			

審査請求 未請求 請求項の数 8 O L (全 6 頁)

(21) 出願番号 特願2000-270016 (P2000-270016)

(22) 出願日 平成12年9月6日 (2000.9.6)

(71) 出願人 000208891

ケイディーディーアイ株式会社
東京都新宿区西新宿二丁目3番2号

(72) 発明者 大岸 智彦

埼玉県上福岡市大原二丁目1番15号 株式
会社ケイディーディ研究所内

(72) 発明者 長谷川 亨

埼玉県上福岡市大原二丁目1番15号 株式
会社ケイディーディ研究所内

(74) 代理人 100078499

弁理士 光石 俊郎 (外2名)

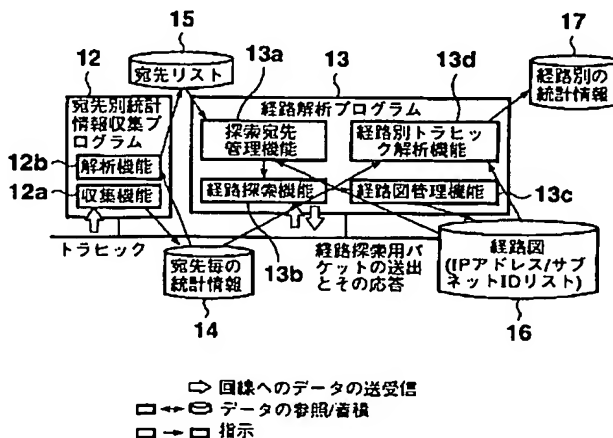
最終頁に続く

(54) 【発明の名称】 経路別トラヒック解析方法

(57) 【要約】

【課題】 経路別にトラヒックを解析すること。

【解決手段】 宛先別統計情報収集プログラム12により、回線上に流れるパケットを監視して宛先別統計情報を収集し、これから宛先リストを抽出する。経路解析プログラム13により、宛先リストに基づいて有用な宛先に対し経路探索を行い、経路探索結果から経路図を作成し、この経路図と宛先別統計情報から経路別の統計情報を導出する。



【特許請求の範囲】

【請求項 1】 経路図及び宛先別統計情報をもとに、経路別の統計情報を導出することを特徴とする経路別トラヒック解析方法。

【請求項 2】 請求項 1 において、前記宛先別統計情報から有用な宛先を複数選択し、選択した宛先について経路探索を行い、得られた複数の経路探索結果から前記経路図を導出することを特徴とする経路別トラヒック解析方法。

【請求項 3】 請求項 2 において、前記有用な宛先の数 10 は前記宛先別統計情報に対応する宛先より少ないことを特徴とする経路別トラヒック解析方法。

【請求項 4】 請求項 2 において、前記有用な宛先として、前記宛先別統計情報からトラヒック量が多い上位複数の宛先、あるいは、品質が悪い上位複数の宛先を選択することを特徴とする経路別トラヒック解析方法。

【請求項 5】 請求項 2 において、同じ経路を持つ宛先の集合についてはそのうち 1 つの宛先のみ経路探索を行うことを特徴とする経路別トラヒック解析方法。

【請求項 6】 請求項 2 において、UDP パケットをそ 20 の IP ヘッド部分の TTL フィールドの値を順次変えて宛先に送信することにより、当該宛先についての経路探索を行うことを特徴とする経路別トラヒック解析方法。

【請求項 7】 請求項 1 において、インターネットサービスプロバイダ内の回線上の 1 点、インターネットサービスプロバイダ間の回線上の 1 点、ユーザ内の回線上の 1 点のうちいずれかにて、回線上を流れるパケットを監視することにより、前記宛先別統計情報を収集することを特徴とする経路別トラヒック解析方法。

【請求項 8】 請求項 1 において、前記経路別の統計情報 30 は、トラヒック量、品質及び経路安定度のうち少なくとも 1 種であることを特徴とする経路別トラヒック解析方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は通信経路別の統計情報を収集し解析する方法に関し、特に、インターネットサービスプロバイダ（以下、ISP (Internet Service Provider: インターネットサービス提供者または設備) 40 と呼ぶ）におけるネットワークの運用に役立つものである。経路別の統計情報としては、トラヒック量（IP バイト数や TCP バイト数など）や品質（再送率やスループットなど）、経路安定度などがある。ネットワークの運用としては、ルーティングポリシーの決定や障害時のルーティングの変更などがある。

【0002】

【従来の技術】下記(1)～(3)に従来技術を示す。

(1) 経路毎の品質測定は、測定用端末から個々の経路のサーバに対して、アクティブにパケットを送信する方法で行われてきた。しかし、この従来技術(1)では、トラ 50

ヒック量を測定することができない。また、厳密な品質測定を行うためには、大量のパケットを送信する必要があるため、ネットワークへの負荷が増大する。

(2) 宛先（IP アドレス）毎にトラヒックを収集する機能を持つツールとして、Cisco 社の Netflow と呼ばれる解析ツールや、Sniffer と呼ばれるプロトコルアナライザがある。しかし、この従来技術(2)では、これらのツールが収集できるのはトラヒック量のみであり、再送量やスループットなどの品質に関する情報、並びに、経路安定度の情報は収集できない。しかも、このような品質に関する情報を収集するには、パケットを収集するとともに、測定用端末内部で TCP コネクションの状態遷移を管理する必要があるが、上記ツールはこれらの機能を持ち合わせていない。また、単に IP アドレス毎の情報からは、経路毎の情報を導出することはできない。

(3) 宛先毎の経路を調査するツールとして、パケットの経路を動的に調べるトレーサルート(traceroute)と呼ばれるソフトウェアがある。しかし、従来技術(3)では、トレーサルートの宛先を選択するメカニズムが提供されていない。なお、従来技術(2)と従来技術(3)を組み合わせたものは知られていないが、仮にこれらを組み合わせてみても、ネットワークへの負荷を減らすために、トレーサルートを行う相手先を制限する必要がある。

【0003】

【発明が解決しようとする課題】本発明の課題は、上述した従来技術の問題点を解消する経路別トラヒック解析方法の提供である。

【0004】

【課題を解決するための手段】請求項 1 に係る発明の経路別トラヒック解析方法は、経路図及び宛先別統計情報をもとに、経路別の統計情報を導出することを特徴とする。請求項 2 に係る発明は、請求項 1 において、前記宛先別統計情報から有用な宛先を複数選択し、選択した宛先について経路探索を行い、得られた複数の経路探索結果から前記経路図を導出することを特徴とする経路別トラヒック解析方法である。

【0005】請求項 3 に係る発明は、請求項 2 において、前記有用な宛先数は前記宛先別統計情報に対応する宛先より少ないことを特徴とする。請求項 4 に係る発明は、請求項 2 において、前記有用な宛先として、前記宛先別統計情報からトラヒック量が多い上位複数の宛先、あるいは、品質が悪い上位複数の宛先を選択することを特徴とする。請求項 5 に係る発明は、請求項 2 において、同じ経路を持つ宛先の集合についてはそのうち 1 つの宛先のみ経路探索を行うことを特徴とする。請求項 6 に係る発明は、請求項 2 において、UDP パケットをその IP ヘッド部分の TTL フィールドの値を順次変えて宛先に送信することにより、当該宛先についての経路探索を行うことを特徴とする。

【0006】請求項 7 に係る発明は、請求項 1 におい

て、インターネットサービスプロバイダ内の回線上の1点、インターネットサービスプロバイダ間の回線上の1点、ユーザ内の回線上の1点のうちいずれかにて、回線上を流れるパケットを監視することにより、前記宛先別統計情報を収集することを特徴とする。請求項8に係る発明は、請求項1において、前記経路別の統計情報は、トラヒック量、品質及び経路安定度のうち少なくとも1種であることを特徴とする。

【0007】

【発明の実施の形態】以下、図面を参照して、本発明の実施形態例を説明する。

【0008】図1において、ユーザ1が同ユーザの所属ISP2からインターネット上のサーバ8、9、10にアクセスする場合、ISP2以降の経路上に種々のISP3、4、5、6、7が存在する。図1の例では、サーバ8への経路はISP3→ISP4→ISP5→サーバ8であり、サーバ9への経路はISP3→ISP4→ISP6→サーバ9であり、サーバ9への経路はISP3→ISP7→サーバ10である。

【0009】そこで、本例では、ISP2がルーティングポリシーの決定や障害時のルーティングの変更などために、ISP2とISP3間の回線上の1点を監視地点11として、経路別のトラヒック量（IPバイト数やTCPバイト数など）、あるいは、経路別の品質（再送率やスループットなど）、あるいは、経路別の経路安定度を解析するものとして説明する。

【0010】また、本例では、コンピュータとその上で動作するコンピュータソフトウェアにより、経路別のトラヒック解析を行うものとする。そのため、コンピュータソフトウェアとして、図2に示すように、宛先別統計情報収集プログラム12と経路解析プログラム13が用いられる。宛先別統計情報収集プログラム12は収集機能12aと、解析機能12bを持つ。経路解析プログラム13は探索宛先管理機能13aと、経路探索機能13bと、経路図管理機能13cと、経路別トラヒック解析機能13dを持つ。また、コンピュータは宛先毎の統計情報を格納する格納部14、宛先リストを格納する格納部15、経路図を格納する格納部16及び経路別の統計情報を格納する格納部17を具える。

【0011】宛先別統計情報収集プログラム12の収集機能12aは、監視地点11にて回線上を流れるパケットを監視し、宛先毎の統計情報を収集し、格納部14に蓄積する。例えば、パケットの発着IPアドレス毎のトラヒックを宛先毎に収集する。ここで、宛先は、発IPアドレスまたは着IPアドレスの一方を表す。

【0012】宛先別統計情報収集プログラム12の解析機能12bは、収集機能12aが収集した宛先毎の統計情報を目的に従って定期的または不定期に解析（ソートやフィルタ等）することにより、有用な複数の宛先からなる宛先リストを作成して格納部15に蓄積する。例え

ば、トラヒック量（IPバイト数またはTCPバイト数）の多い順に宛先を並び替え、トラヒック量が多い上位n個の宛先のみを選択し、あるいは、品質（再送率またはスループット）の悪い順に宛先を並び替え、品質が悪い上位n個の宛先のみを選択し、宛先リストとして抽出する。ここで、nは複数であるが、その値は監視地点11における経路探索用トラヒックの許容量に合わせて調整する。つまり、宛先数が多いほどより多数且つ正確な経路別トラヒックが得られる反面、経路探索用トラヒックが増大する。

【0013】トラヒック量が多い宛先のみを選択した場合は、ユーザが多く利用している経路を対象としてトラヒック解析を行うことになる。従って、実際に多く利用されている経路ほど、より正確な経路別トラヒックの解析結果が得られる。

【0014】一方、品質が悪い宛先のみを選択した場合は、ユーザに品質の劣化を与えている経路におけるトラヒック量、品質、経路安定度の情報を、より詳細に解析することができる。また、トラヒック量に比べて帯域が狭い回線など、特定の経路における問題点を推定することが可能となる。

【0015】経路解析プログラム13の探索宛先管理機能13aは、格納部15に蓄積された宛先リストに基づくだけでなく、格納部16に蓄積された経路図にも基づいて、経路探索を行うべき宛先を決定する。宛先の決定は以下の方針①②で行う。

①同じ経路を持つ（サーバ）の集合（サーバ群）からは、1つの宛先（サーバ）のみを選択する。

②サーバ群に含まれるサーバの管理は、経路図管理機能13bで行われる。

【0016】経路解析プログラム13の経路探索機能13bは、複数の宛先に対して経路探索を実行し、探索完了までの状態を管理する。経路探索にはトレースルート(traceroute)と同様の方式を用いる。具体的には、個々の宛先に対する経路探索は以下の手順(1)～(10)で実行する。

(1) 最初はIPパケットのTTL(time to live : タイム・トゥ・ライブ (生存時間)) フィールドの値を1とし、UDP (ユーザ・データグラム・プロトコル) パケットを送信する。なお、TTLフィールドのデフォルト値は32である。

(2) パケットを中継するルータはTTLフィールドを1減らす。このとき、TTLフィールドが0より大きいときは、そのルータが管理するルーティングテーブルを参照し、次のホップを調べる。

(3) 次のホップがルータの場合は、そのルータへの中継を行う。次のホップがホスト、つまり最終宛先の場合はその宛先へUDPパケットを転送する。

(4) TTLフィールドが0となった場合には、中継できないと判断し、TTLフィールドが0になったルータか

ら、発信元にエラーパケットの 1 種である ICMP (インターネット・コントロール・メッセージ・プロトコル) のタイム・エクシーデッド(time exceeded) パケットが送信される。

(5) 最終的な宛先からは、ICMP のポート・アンリーチャブル(port unreachable)パケットが送信される。これは、トレースルートで用いられる UDP パケットは、通常端末がサポートしないポート番号を使用するためである。

(6) 最終的な宛先に届く前に TTL フィールドの値が 0 になってしまった場合は、上記手順(1)に戻って TTL を 1 増加して、再び発信元から UDP パケットを送信する。

(7) 以上の手順(1)～(6)を UDP パケットが最終的な宛先に届くまで繰り返す。

(8) 以上の手順(1)～(7)により、図 3 に示すように、発信元 ISP 2 から宛先のサーバ 10 までのルータ 18、19、20 の経路が判る。

(9) そこで、経路上の各ルータ 18、19、20 に対し、DNS (ドメイン・ネーム・システム) によるドメイン探索を行い、各ルータ 18、19、20 を管理するドメインを調査する。つまり、各ルータ 18、19、20 の IP アドレスからそれぞれのドメイン名を探索する。ドメインとしては、ドメイン間の中継を行うドメインと、中継を行わないドメインとを区別する。これらの区別は、ドメイン識別により行う。ここでは、中継を行うドメインを ISP と呼ぶ。一般に、.com はサーバ、.net は ISP である。

(10) 経路上に同一のドメインが存在する場合は、それらを集約する。図 4 に示す例では、ルータ 18 とルータ 19 は aaa.net という同一のドメイン名であるので、同一ドメイン内のルータであると判断でき、1 つのドメイン (図 1 に対応させれば ISP 3) となる。ルータ 20 は ISP 7 に相当する。中継を行わないドメインがある場合は、それらを最終宛先として集約する。

【0017】経路解析プログラム 13 の経路図管理機能 13c は、経路探索機能 13b により得られた複数の宛先に対する探索結果を元に、経路図を作成し格納部 16 に蓄積する。その際、同一経路となる複数のサーバは、サーバ群として集約する。サーバ群の情報としては、IP アドレスと、IP アドレスを集積して得られたサブネット ID のリストを管理する。経路図は、監視地点 11 (ISP 内あるいは ISP 間あるいはユーザ内の回線上の 1 点) から複数の宛先までの ISP の経路 (ISP の接続) をツリー上に構成したものである。図 1 のような ISP のツリーからなる経路図である。また、経路図におけるツリーの末端、つまり、最終宛先には、複数の宛先がリスト上に並ぶ。

【0018】経路解析プログラム 13 の経路別トラヒック解析機能 13d は、格納部 14 に蓄積された宛先別統

計情報と格納部 16 に蓄積された経路図を用いて、統計情報を宛先別から経路別に組み換えることにより、経路別の統計情報を導出し、格納部 17 に蓄積する。

【0019】なお、経路安定度については、経路は常に安定しているとは限らないので、同一宛先に対して時刻を変えて経路探索を行い、経路探索の変動を監視することにより、経路別の経路安定度を収集することができる。

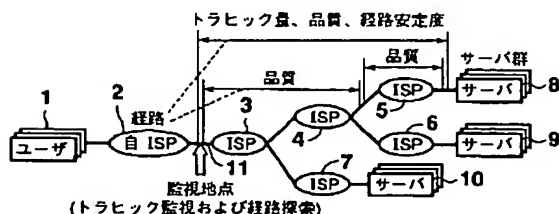
【0020】本例では監視地点 11 をインターネットサービスプロバイダ内の回線上の 1 点としたが、インターネットサービスプロバイダ間の回線上の 1 点、あるいは、ユーザ内の回線上の 1 点とすることができる。

【0021】上述のように、経路図と宛先別統計情報をもとに経路別の統計情報を導出することにより、経路別にトラヒックを解析することができる。また、経路図は、宛先別統計情報から宛先を複数選択し、選択した宛先について経路探索を行うことにより、得られた複数の経路探索結果から導出することができる。この場合、経路探索を行う宛先として有用なもののみを選択することにより、経路別トラヒック解析に実用上十分な経路探索を行うことができると共に、経路探索用トラヒックがネットワークへ与える負荷を減らすことができる。従って、通常は、有用な宛先の数は宛先別統計情報に対応する宛先より少なくされる。特に、有用な宛先として、宛先別統計情報からトラヒック量が多い上位複数の宛先、あるいは、品質が悪い上位複数の宛先を選択することにより、実用上十分な経路別トラヒック解析を行うことができる。また、同じ経路を持つ宛先の集合についてはそのうち 1 つの宛先のみ経路探索を行うことにより、経路探索用トラヒックがネットワークへ与える負荷を減らすことができる。経路探索には任意の経路探索ツールを使用できるが、UDP パケットをその IP ヘッド部分の TTL フィールドの値を順次変えて宛先に送信して当該宛先についての経路探索を行うという、トレースルート (traceroute) と同様の方式を用いることにより、簡便に経路探索を行うことができる。更に、本発明で解析する経路別統計情報として、トラヒック量、品質及び経路安定度のうち少なくとも 1 種を対象とすることができる。また、トラヒック量としては IP バイト数や TCP バイト数などがあり、品質としては再送率やスループットなどがある。

【0022】上述した本例の統計別トラヒック解析方法を実現する装置構成について説明すると、同統計別トラヒック解析装置は各種の格納部 14～17 に加えて、コンピュータと宛先別統計情報収集プログラム 12 により実現される宛先別統計情報収集装置と、コンピュータと経路解析プログラム 13 により実現される経路解析装置を具える。宛先別統計情報収集装置は収集機能部と解析機能部を持ち、経路解析装置は探索宛先管理機能部と、経路探索機能部と、経路図管理機能部と、経路別トラヒ

(1) あるISP内の回線上の1点、あるいは、ISP間の回線上の1点、あるいは、あるユーザ内の回線上の1点で監視することにより、監視地点のパケット経路が同じサーバ群へのトラフィック量（IPバイト数やTCPパ

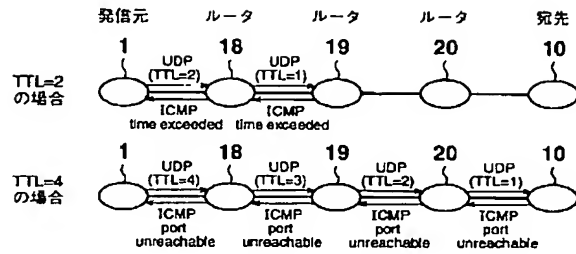
経路別に解析される情報



- 1 ユーザ
- 2 ～ 7 I S P
- 8 ～ 1 0 サーバ
- 1 1 監視地点
- 1 2 宛先別統計情報収集プログラム
- 1 2 a 収集機能
- 1 2 b 解析機能
- 1 3 経路解析プログラム
- 1 3 a 探索宛先管理機能
- 1 3 b 経路探索機能
- 1 3 c 経路図管理機能
- 1 3 d 経路別トラヒック解析機能
- 1 4 宛先別統計情報格納部
- 1 5 宛先リスト格納部
- 1 6 経路図格納部
- 1 7 経路別統計情報格納部
- 1 8、1 9、2 0 ルータ

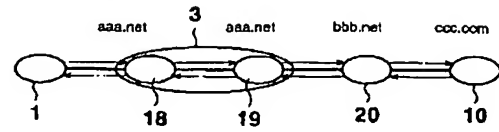
【図 3】

tracerouteの方式



【図 4】

ドメインの接続



フロントページの続き

(72)発明者 中尾 康二
 埼玉県上福岡市大原二丁目 1 番15号 株式
 会社ケイディディ研究所内

Fターム(参考) 5K019 BB22 DB08 DC01 DC06
 5K030 HA08 JA10 MB04 MB09 MC03
 MC07